RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: SBV-W02

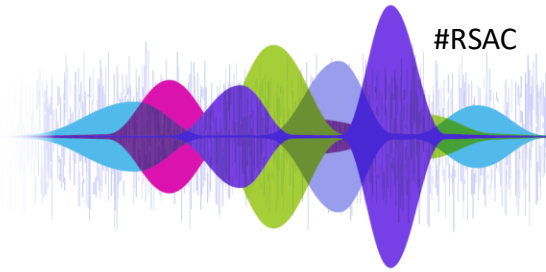
Building Cyber Defenses to Withstand Sophisticated Cyber Adversaries

MODERATOR: **Abhijith 'Abx' B Rs**
Founder at Adversary Village
Founder & Head of Security Consulting at BreachSimRange
in.linkedin.com/in/abhijith-b-r

PANELISTS: **Jonathan Baker**
Director, Center for Threat-Informed Defense, MITRE
linkedin.com/in/jonathanobaker

Vivek Ramachandran
Founder and CEO at SquareX
linkedin.com/in/vivekramachandran

Ken Kato
Chief Security Officer at Kindo
linkedin.com/in/devsecops-kkato



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

#RSAC

Many Voices.
One Community.

MODERATOR:

Abhijith ‘Abx’ B R

Founder at Adversary Village
Head of Security Consulting at BreachSimRange
in.linkedin.com/in/abhijith-b-r

PANELISTS:

Jon Baker

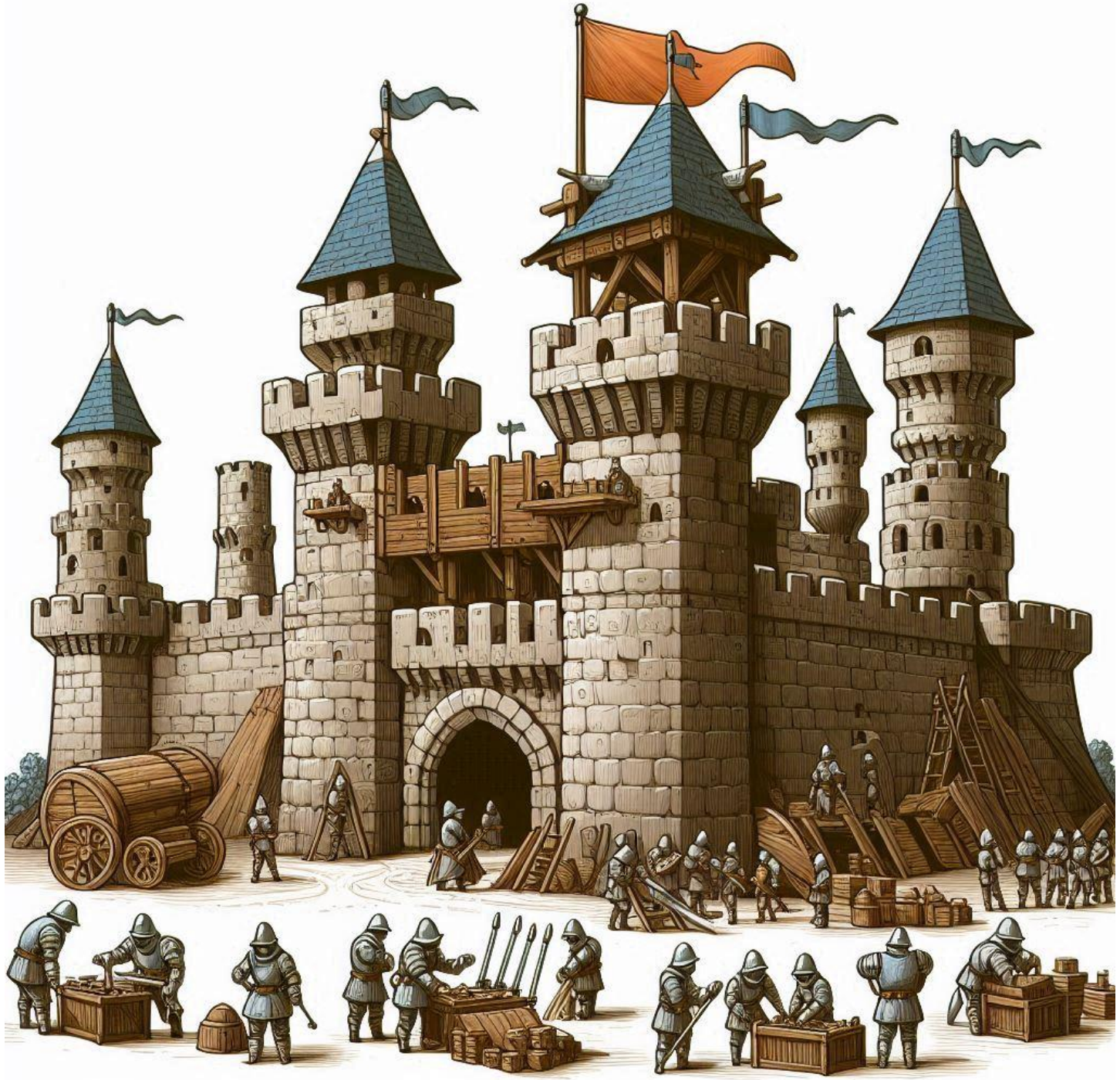
Director, Center for Threat Informed Defense, MITRE
linkedin.com/in/jonathanobaker

Vivek Ramachandran

Founder and CEO at SquareX
linkedin.com/in/vivekramachandran

Ken Kato

Chief Security Officer at Kindo
linkedin.com/in/devsecops-kkato



How to build your fortress to withstand sophisticated attackers

Sophisticated cyber adversaries

- Cyber-attacks ranging from sophisticated ransomware to state-sponsored attacks, charging against your organizations.
  - Sophisticated, how?
  - Ransomware as a service
  - State-sponsored cyber threat actors
  - Key breaches and incidents of 2024

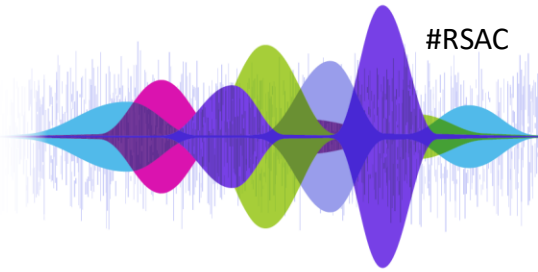
Breaching the defenses

- Cyber adversaries are successfully gaining initial access to even well-established organizations, despite the presence of multiple security products and defenses.
- How does it happen?

Initial access attack vectors

- Initial access attack vectors and how adversaries gain access bypassing modern security controls
  - Notable initial access tools, techniques used by adversaries
  - Initial access brokers
  - How threat actors are evading modern security controls and defense systems for gaining access
  - What are we missing as a defender?

Generative AI for offensive operations

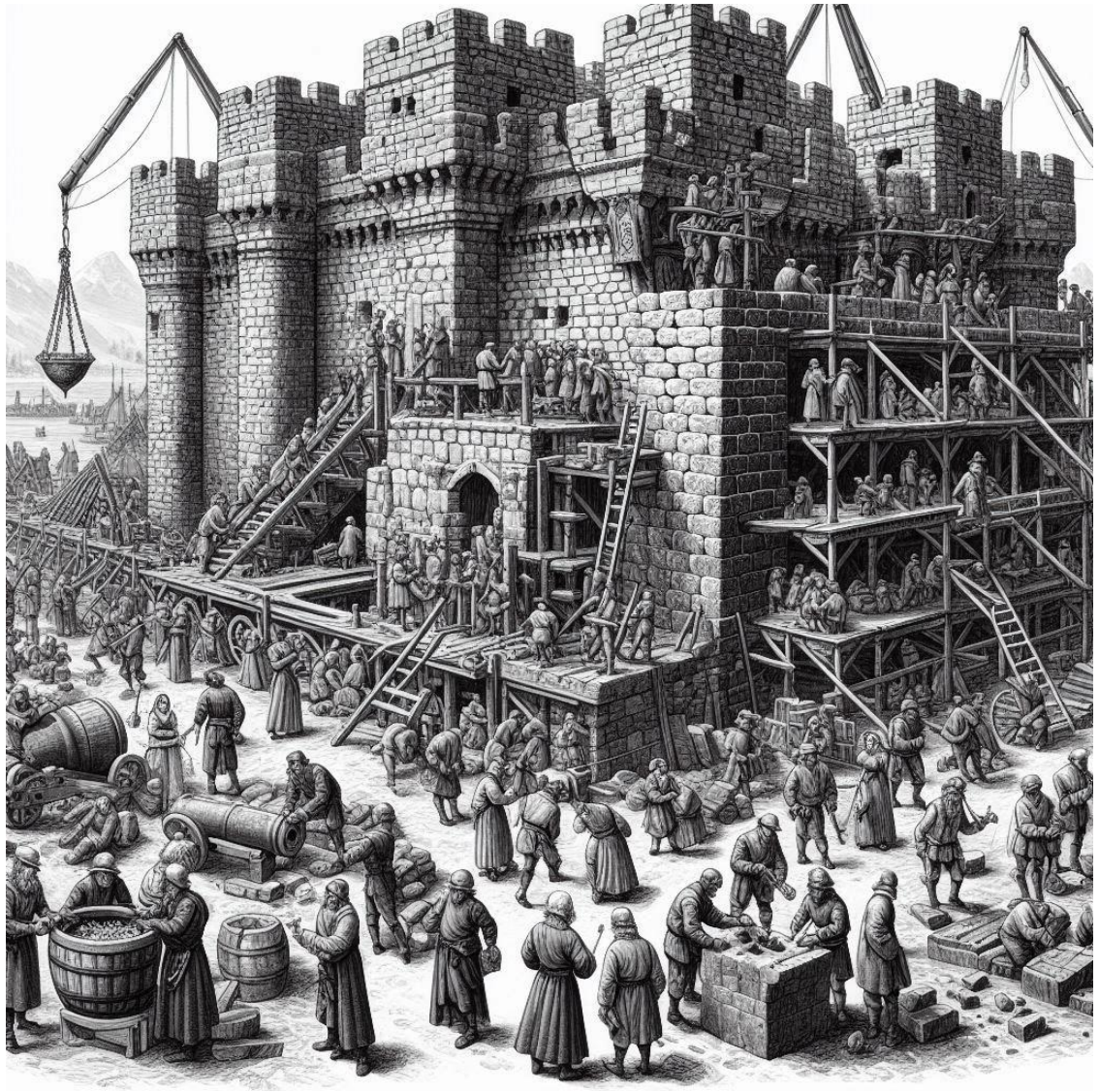


- Attacks using AI systems and leveraging uncensored AI for offensive operations
  - Incidents of cyber threat-actors using AI systems to craft better payloads and techniques
  - Using generative AI systems for the betterment of defensive/offensive systems and controls
- Attacks against AI systems?
  - Adversaries fooling AI systems to breach sensitive data and gain access?

Building defenses == building offensive teams?

- How offensive security operations and adversary simulation can be helpful to organization to build better defenses
- Key concepts of adversary attack simulation
  - Adversary Simulation Vs. Adversary Emulation
  - Threat-Informed Defense
  - Adversarial Exposure Validation
  - Dynamic red teaming and adversary simulation

Building defenses



- Building and finetuning cyber defenses to withstand sophisticated cyber adversaries
  - Deploying security products with continuous control validation in mind
  - Adversarial exposure testing on the principle of People, Process and Technology
  - Threat-Intel powered continuous threat and adversary emulation
  - Dynamic adversarial attack simulation to test defenses
  - A bullet proof incident response plan

Building your cyber defenses to withstand sophisticated cyber adversaries

Apply What You Have Learned Today

- Next week you should:
  - Identify cyber threat actors and adversary groups targeting your organization and industry
- In the first three months following this panel you should:
  - Initiating small adversary emulation campaigns against endpoint security controls and products
  - Evaluate how the defenses improved post continuous testing
- Within six months you should:
  - Build a security initiative using threat-informed defense and continuous adversary emulation as the foundation
  - Drive security control validation assessment against the security products deployed in your organization, process and policies
  - Address the gaps, continuous betterment of defense systems

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You